

Notice of Allowability

Application No.

10/074,804

Examiner

Longbit Chai

Applicant(s)

GARCIA, DENIS JACQUES PAUL

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to phone interview on 7/27/2007.
2. ☒ The allowed claim(s) is/are 1-39.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).


* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 7/27/2007.
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/11/2007 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Glenn J. Perry (Reg. No. 28,458) on 7/27/2007.

This application has been amended as follows:

IN THE CLAIMS

Replace claim 1 – 6, 9, 11, 13, 16, 17, 25, 28 and 33 – 39 as follows.

Art Unit: 2131

Claim 1:

A system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, comprising:

a client-module configured to generate a header comprising a plurality of one or more sets of encrypted security information corresponding to respective one of a plurality of groups of users, wherein the encrypted security information comprises a file key and access rules to control the restricted access to the electronic data as to who and how a file including the electronic data can be accessed, and configured to generate an encrypted data portion comprising the file encrypted with one or more a plurality of file keys, each of the file keys corresponding to each of the sets according to a predetermined cipher scheme, wherein the header is associated with ~~coupled to~~ the encrypted data portion to generate a secured file, ~~each set of the one or more sets of encrypted security information associated with a designated group of users; and~~

a server-module configured to obtain a respective one of the file keys ~~file key~~ associated with a corresponding one of the plurality of groups ~~the designated group of users~~ and to decrypt ~~only a the~~ set of the plurality of one or more sets of encrypted security information associated with the respective one of the groups ~~designated group of users~~ to allow access by the respective one of the groups according to the access rules ~~designated group of users;~~

a module configured to retrieve the respective one of the file keys from a memory store if the secured file is newly generated and the secured file is being stored in a storage place; and a module configured to delete the one or more file keys from a memory store as soon as the newly generated secured file is stored in the storage place.

Claim 2:

The system as recited in Claim 1, wherein the plurality of one or more sets of encrypted security information in the header of the secured file facilitates the restricted access to the file.

Art Unit: 2131

Claim 3:

The system as recited in Claim 1, wherein the plurality of one or more sets of security information is encrypted with a key from the plurality of one or more file keys associated with the one of a plurality of groups ~~the designated group~~ of users.

Claim 4:

The system as recited in Claim 3, wherein the one of a plurality of groups ~~the designated group of users~~ includes one or more of ~~selected from a group consisting of a human users, a software agents, and a devices and a group of users;~~ and wherein the one of a plurality of groups ~~the designated group~~ of users is granted access privilege to access the file.

Claim 5:

The system as recited in Claim 4, wherein the plurality of one or more sets of encrypted security information comprises one of the plurality of ~~the~~ file keys and access rules to the restricted access to the file.

Claim 6:

The system as recited in Claim 5, wherein the file key is retrieved to decrypt the encrypted data portion in the secured file when the access privilege of the one of a plurality of groups ~~the designated group~~ of users is ~~within~~ consistent with access permissions by the access rules.

Claim 9:

Art Unit: 2131

The system as recited in Claim 7, wherein the markup language ~~is~~ includes one or more ~~selected from a group consisting of~~ HTML, XML, and SGML.

Claim 11:

The system as recited in Claim 10, wherein each of the plurality of ~~one or more sets~~ of encrypted security information comprises a flag to the application that the secured file being accessed can not be accessed as it is normally accessed ~~does~~.

Claim 13:

The system as recited in Claim 10, wherein each of the plurality of ~~one or more sets~~ of encrypted security information comprises the file key and access rules, the access rules controlling who and how the secured file can be accessed, and wherein the security information in the header is organized in such a way that the application is paused, upon detecting that the secured file is being accessed, for an access control module to determine whether the one of a plurality of groups ~~the designated group~~ of users requesting the secured file has proper access privileges to do so with respect to the access rules in the security information.

Claim 16:

The system as recited in Claim 1, wherein the electronic data file ~~is~~ one or more of an electronic document, a multimedia file, ~~a set of~~ dynamic or static data, ~~a sequence of~~ executable code, an image file, streaming audio, streaming video, executable code, audio files, databases, database tables, database table records, collections of electronic files; and collections of electronic documents ~~and a text data~~.

Art Unit: 2131

Claim 17:

A system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, comprising:

a ~~client~~-module configured to generate a header including an plurality of encrypted file keys and a rule block having N encrypted segments, each of the N encrypted segments including a ~~set of~~ plurality of access rules facilitating the restricted access to a file including the electronic data, wherein $N \geq 1$ and an encrypted data portion including the electronic data encrypted according to a predetermined cipher; ~~and~~

wherein the header is associated with ~~coupled to~~ the encrypted data portion to generate a secured file, and the file key can be retrieved to decrypt the encrypted data portion only when one of the respective plurality of access rules in one of the N encrypted segments are measured successfully against access privileges associated with a one of a respective plurality of groups of designated users accessing the secured file;

a module configured to retrieve the respective one of the file keys from a memory store if the secured file is newly generated and being stored in a storage place; and

a module configured to delete the one or more file keys from a memory store as soon as the newly generated secured file is stored in the storage place.

Claim 25:

The system as recited in Claim 24, wherein the action comprises one or more of ~~commands: open, export, read, edit, play, listen to, or print or forward and attach.~~

Claim 28:

The system as recited in Claim 26, wherein the markup language is one or more ~~selected from a group consisting of~~ HTML, XML, and SGML.

Art Unit: 2131

Claim 33:

In a system for providing access control management to electronic data, wherein the electronic data is structured in a format that provides restricted access to the electronic data therein, a method for generating the format, comprising:

obtaining one of a plurality of file keys;

encrypting the electronic data with one of a plurality of the file keys according to a predetermined cipher to produce an plurality of encrypted data portions; ~~and~~

integrating a header comprising a plurality of one or more sets of encrypted security information with the encrypted data portion to generate a secured file, wherein the encrypted security information comprises the file key and access rules to control the restricted access to the electronic data in the secured file, each set of the plurality of one or more sets of encrypted security information associated with a corresponding one of a plurality of groups a designated group of users;

if the secured file is being stored in a storage place, retrieving the file key from a memory store; and

deleting the file key from a memory store as soon as the secured file is stored in the storage place.

Claim 34:

The method of Claim 33, wherein the encrypted security information comprises user information as to which of the corresponding one of a plurality of groups a designated group of users can access the secured file.

Claim 35:

The method of Claim 34, wherein the plurality of one or more sets of encrypted security information can only be decrypted by a key associated with the corresponding one of a plurality of groups a designated group of users identified in the user information in the plurality of one or more sets of encrypted security information.

Art Unit: 2131

Claim 36:

The method of Claim 34, wherein the corresponding one of a plurality of groups a designated group of users includes one or more ~~is a member selected from a group consisting of a human users, a software agents, and a devices and a group of users;~~ and wherein the users are ~~is granted access privileges~~ to access the secured file.

Claim 37:

The method of Claim 36 further comprising obtaining the access rules from either a default setting for a file place in which the secured file is to be placed or a manual setting in accordance with access privilege associated with a user from the corresponding one of a plurality of groups ~~a designated group of users~~ who is creating the secured file.

Claim 38:

The method of Claim 33, wherein the obtaining of the file key comprises:
if the secured file is newly generated, generating the file key from the predetermined cipher; ~~and if the secured file is being stored in a storage place, retrieving the file key from a memory store; and~~
~~deleting the file key from a memory store as soon as the secured file is stored in the storage place.~~

Claim 39:

The method of claim 1, wherein each of the corresponding one of a plurality of groups a designated group of users has different access privileges.

Allowable Subject Matter

1. Claims 1 – 39 are allowed.
2. The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations, as recited in independent claims 1, 17 and 33 (& associated dependent claims).

The prior arts fail to teach or suggest a system for providing access control management configured to generate a header with a plurality of sets of encrypted security information corresponding to respective one of a plurality of groups of users having a file key and access rules to control the restricted access to the electronic data and configured to generate an encrypted data portion encrypted with a plurality of file keys, each of the file keys corresponding to each of the sets, wherein the header is associated with the encrypted data portion to generate a secured file; a module configured to obtain a respective one of the file keys associated with a corresponding one of the plurality of groups and to decrypt the set of the plurality of sets of encrypted security information associated with the respective one of the groups to allow access by the respective one of the groups according to the access rules; a module configured to retrieve the respective one of the file keys from a memory store if the secured file is newly generated and the secured file is being stored in a storage place; and a module configured to delete the one or more file keys from a memory store as soon as the newly generated secured file is stored in the storage place.

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

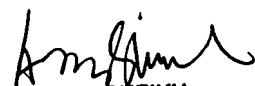
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai

Examiner

Art Unit 2131


LBC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100